

FOR IMMEDIATE RELEASE THURSDAY, OCTOBER 11, 2007 WWW.USDOJ.GOV NSD (202) 514-2007 TDD (202) 514-1888

JUSTICE DEPARTMENT AND PARTNER AGENCIES LAUNCH NATIONAL COUNTER-PROLIFERATION INITIATIVE

WASHINGTON, D.C. — The Justice Department and several partner agencies today launched a national initiative that will harness the counter-proliferation assets of U.S. law enforcement, licensing, and intelligence agencies to combat the growing national security threat posed by illegal exports of restricted U.S. military and dual-use technology to foreign nations and terrorist organizations.

The export enforcement initiative was announced by Kenneth L. Wainstein, Assistant Attorney General for National Security; Julie L. Myers, Homeland Security Assistant Secretary for U.S. Immigration and Customs Enforcement (ICE); Timothy D. Bereznay, Assistant Director, FBI Counterintelligence Division; Darryl W. Jackson, Assistant Secretary of Commerce for Export Enforcement; Charles W. Beardall, Director of the Defense Criminal Investigative Service (DCIS); and Stephen D. Mull, Acting Assistant Secretary of State for Political Military Affairs.

The threat posed by illegal foreign acquisition of restricted U.S. technology is substantial and growing. In the past week, there have been federal cases involving the illegal export of items with nuclear and missile applications to Pakistan and the illegal export of U.S. fighter jet components sought by Iran. A 2006 Defense Department report noted a 43 percent increase in the number of suspicious foreign contacts with U.S. defense firms, and an Intelligence Community report issued last year asserted that entities from a record 108 nations were engaged in efforts to obtain controlled U.S. technology.

China and Iran pose particular U.S. export control concerns. The majority of U.S. criminal export prosecutions in recent years have involved restricted U.S. technology bound for these nations as opposed to others. Recent prosecutions have highlighted illegal exports of stealth missile technology, military aircraft components, Naval warship data, night vision equipment, and other restricted technology destined for China or Iran.

"Foreign states and terrorist organizations are actively seeking to acquire U.S. data, technological knowledge and equipment that will advance their military capacity, their weapons systems and even their weapons of mass destruction programs. Many have targeted our government, industries and universities as sources of these materials," said Assistant Attorney General Wainstein. "This initiative is a coordinated campaign to keep

sensitive U.S. technology from falling into the wrong hands and from being used against our allies, against our troops overseas or against Americans at home."

New Counter-Proliferation Task Forces and Training

A critical part of this new initiative will be the formation of Counter-Proliferation Task Forces in appropriate U.S. Attorney's offices around the country. These multiagency task forces will take many of the concepts used in combating terrorism – namely, prevention, cooperation and coordination — and apply them to the counter-proliferation effort. The task forces will be designed to enhance cooperation among all agencies involved in export control, forge relationships with affected industries, and facilitate information sharing to prevent illegal foreign acquisition of U.S. technology.

The Department's National Security Division is in discussions with districts with large concentrations of high-tech businesses and research facilities -- all of which are potential targets for illegal foreign acquisition efforts -- as potential venues for new task forces. Some task forces may be modeled after efforts that exist in the Southern District of New York, District of Connecticut and District of Maryland, where agents from ICE, FBI, Commerce Department, DCIS and other agencies pool data and coordinate cases. Other approaches may be taken in different districts, depending on the needs of the U.S. Attorney and agencies in that district.

The new initiative also includes key training components. Export prosecutions are by nature complex because they involve intricate laws, sensitive international issues, agencies with different authorities, and, often, classified information. Under the initiative, the Department will provide specialized training to its field prosecutors, especially those with limited expertise in export control. The Department launched this enhanced training effort in May with a national conference in South Carolina.

The Justice Department has also appointed its first National Export Control Coordinator to implement this initiative and foster coordination among the agencies involved in export control. Based in the Counterespionage Section of the National Security Division, the Coordinator is responsible for managing the nationwide training of prosecutors and monitoring progress on export control prosecutions around the country.

Improved Coordination With Export Licensing Agencies

A final component of the initiative involves greater coordination between the Justice Department and the export licensing agencies, particularly the State Department's Directorate of Defense Trade Controls and the Commerce Department's Bureau of Industry and Security. As part of the initiative, the Justice Department's National Security Division has initiated monthly meetings with the leadership of these offices to ensure that investigations, prosecutions and enforcement issues are fully coordinated.

"These crimes result in some of the most complex and time-consuming cases facing federal law enforcement," said Julie L. Myers, Homeland Security Assistant

Secretary for ICE. "The concept of terrorists, criminals or rogue nations obtaining weapons and other restricted technology is chilling. By harnessing our collective authorities and efforts, we are better able to protect our national security and global public safety."

According to Timothy D. Bereznay, Assistant Director, FBI Counterintelligence Division, "The FBI is committed to working with our law enforcement and intelligence partners in the aggressive pursuit and investigation of high technology export violations. The theft of intellectual property and technology by foreign parties or governments directly threatens both the national and economic security of the U.S. in which the development and manufacturing of U.S. products results in weakened economic capability and diminished political stature for this country."

"I commend Assistant Attorney General Wainstein and the Department of Justice for their leadership on the Export Enforcement Initiative," said Commerce Assistant Secretary for Export Enforcement Darryl W. Jackson. "This initiative enhances the administration's counter-proliferation program by vigorously pursuing and prosecuting individuals who violate our laws and allow U.S. technology to fall into the wrong hands."

"There are few greater threats to our soldiers, sailors, airmen, and marines than confronting highly-advanced weapons and technology which were designed to protect them and to give them the advantage on the battlefield. It is clear then why the Defense Criminal Investigative Service has for years made illegal technology export a top investigative priority. Our agents, who are dedicated to protecting America's Warfighters, need no motivation in aggressively pursuing these criminals. This initiative is vital and has our full support," said DCIS Director Charles W. Beardall.

"As head of the U.S. Government agency responsible for controlling the export of U.S. defense articles and services, I am delighted to lend my full support to the Export Enforcement Initiative. The Department of State has always maintained a close, working relationship with the federal law enforcement community in its investigation and prosecution of criminal violations of our nation's export control laws. We expect that relationship to only become stronger under this initiative to keep sensitive defense items out of the wrong hands," said Acting Assistant Secretary of State Stephen D. Mull.

Foreign Efforts to Obtain Controlled U.S. Technology

The technology at the heart of this initiative includes restricted U.S. military items, dual-use equipment, and other technical expertise or know-how, some of which have applications in Weapons of Mass Destruction (WMD). These materials are generally restricted and may not be exported without U.S. government approval. Foreign procurement networks intent on obtaining such materials from the U.S. rarely target complete weapons systems, but often focus on seemingly innocuous components to develop their own weapons systems. Two cases in the past week are exemplary:

- *Nuclear-Related Technology to Pakistan*: On Oct. 4, 2007, a Pittsburgh company called SparesGlobal, Inc. was sentenced in the Western District of Pennsylvania for conspiring to make false statements about an illegal export of graphite products that can be used in nuclear reactors and in the nose cones of ballistic missiles. These sensitive products ended up in Pakistan after being routed through the United Arab Emirates. The investigation was conducted by Commerce Department agents.
- *Illegal Exports of U.S. Fighter Jet Components*: On Oct. 5, 2007, Abraham Trujillo and David Wayne were charged in the District of Utah with attempting to illegally export restricted components for F-4 and F-14 fighter jets. Such exports are of particular concern because F-14 components are widely sought by Iran, which is currently the only government in the world that still flies the F-14 fighter jet. The investigation was conducted by ICE and DCIS agents.

According to the Intelligence Community's most recent report to Congress on Foreign Economic Espionage and Industrial Collection, private-sector businessmen, scientists, students, and academics from overseas are among the most active collectors of sensitive U.S. technology. Most did not initially come to the U.S. with that intent, nor were they directed to do so by foreign governments. Instead, after finding that they had access to technology in demand overseas, they engaged in illegal collection to satisfy a desire for profits, acclaim, or patriotism to their home nations.

At the same time, foreign government organizations remain aggressive in illegally acquiring sensitive U.S. technology. Some governments have established quasi-official organizations in the U.S. to facilitate contact with overseas scientists, engineers and businessmen. Foreign governments have been observed directly targeting U.S. firms; employing commercial firms in the U.S. and third countries to acquire U.S. technology; and recruiting students, professors, and scientists to engage in technology collection.

Enhanced U.S. Law Enforcement Response

In addressing such threats, law enforcement agencies and federal prosecutors have stepped their enforcement activity in recent years. ICE has recently doubled the number of agents assigned to export control cases and reports making 149 export-related arrests last fiscal year. The FBI reports that it is investigating roughly 125 economic espionage cases and has increased counterintelligence instruction for new agents by 240 percent.

The Commerce Department reports that more than 80 percent of its export convictions in fiscal year 2007 were related to WMD proliferation, terrorist support or diversion to military end-use. DCIS and other Defense Department agencies have also stepped up their investigative efforts to protect critical military technologies. As a result, the Justice Department has seen a corresponding surge in export prosecutions. In fiscal year 2007, there was more than a 50 percent increase in defendants charged with violating the primary export control statutes compared to the prior year.

###

07-806